

## HTTP Request

```
Frame 15957: 293 bytes on wire (2344 bits), 293 bytes captured (2344 bits) on interface \Device\NPF {122242F4-49BC-4798-8231-1C1E26995AEF}, id 0
Ethernet II, Src: ASUSTekCOMPU_ae:9f:e9 (c8:7f:54:ae:9f:e9), Dst: TPLink_de:71:a5 (78:8c:b5:de:71:a5)
Internet Protocol Version 4, Src: 192.168.0.5, Dst: 23.36.25.85
Transmission Control Protocol, Src Port: 51357, Dst Port: 80, Seq: 1, Ack: 1, Len: 239
Hypertext Transfer Protocol
```

## 2. Data Link Layer

```
Ethernet II, Src: ASUSTekCOMPU_ae:9f:e9 (c8:7f:54:ae:9f:e9), Dst: TPLink_de:71:a5 (78:8c:b5:de:71:a5)
  Destination: TPLink_de:71:a5 (78:8c:b5:de:71:a5)
    Address: TPLink_de:71:a5 (78:8c:b5:de:71:a5)
      .... ..0. .... = LG bit: Globally unique address (factory default)
      .... ..0. .... = IG bit: Individual address (unicast)
  Source: ASUSTekCOMPU_ae:9f:e9 (c8:7f:54:ae:9f:e9)
    Address: ASUSTekCOMPU_ae:9f:e9 (c8:7f:54:ae:9f:e9)
      .... ..0. .... = LG bit: Globally unique address (factory default)
      .... ..0. .... = IG bit: Individual address (unicast)
  Type: IPv4 (0x0800)
```

Here, we can see,

Src Mac address: c8:7f:54:ae:9f:e9

Dst Mac address: 78:8c:b5:de:71:a5

And the type is IPv4

## 3. Network Layer

```
Internet Protocol Version 4, Src: 192.168.0.5, Dst: 23.36.25.85
  0100 .... = Version: 4
  .... 0101 = Header Length: 20 bytes (5)
  Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    0000 00.. = Differentiated Services Codepoint: Default (0)
    .... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
  Total Length: 279
  Identification: 0xd2e9 (53993)
  010. .... = Flags: 0x2, Don't fragment
    0... .... = Reserved bit: Not set
    .1.. .... = Don't fragment: Set
    ..0. .... = More fragments: Not set
    ...0 0000 0000 0000 = Fragment Offset: 0
  Time to Live: 128
  Protocol: TCP (6)
  Header Checksum: 0x0000 [validation disabled]
  [Header checksum status: Unverified]
  Source Address: 192.168.0.5
  Destination Address: 23.36.25.85
```

Here we can see,

This is IP version 4

The source IP address: 192.168.0.5

The destination IP address: 23.36.25.85

This is using TCP and the protocol number 6 in the IP header.

## 4. Transport Layer

```

- Transmission Control Protocol, Src Port: 51357, Dst Port: 80, Seq: 1, Ack: 1, Len: 239
  Source Port: 51357
  Destination Port: 80
  [Stream index: 143]
  - [Conversation completeness: Complete, WITH_DATA (31)]
    ..0. .... = RST: Absent
    ...1 .... = FIN: Present
    .... 1... = Data: Present
    .... .1.. = ACK: Present
    .... ..1. = SYN-ACK: Present
    .... ...1 = SYN: Present
    [Completeness Flags: ·FDASS]
    [TCP Segment Len: 239]
    Sequence Number: 1      (relative sequence number)
    Sequence Number (raw): 1019411586
    [Next Sequence Number: 240      (relative sequence number)]
    Acknowledgment Number: 1      (relative ack number)
    Acknowledgment number (raw): 2706884587
    0101 .... = Header Length: 20 bytes (5)
  - Flags: 0x018 (PSH, ACK)
    000. .... .... = Reserved: Not set
    ...0 .... .... = Accurate ECN: Not set
    .... 0... .... = Congestion Window Reduced: Not set
    .... .0.. .... = ECN-Echo: Not set
    .... ..0. .... = Urgent: Not set
    .... ...1 .... = Acknowledgment: Set
    .... .... 1... = Push: Set
    .... .... .0.. = Reset: Not set
    .... .... ..0. = Syn: Not set
    .... .... ...0 = Fin: Not set
    [TCP Flags: .....AP...]
    Window: 1026
    [Calculated window size: 262656]
    [Window size scaling factor: 256]
    Checksum: 0xf22f [unverified]
    [Checksum Status: Unverified]
    Urgent Pointer: 0
  - [Timestamps]
    [Time since first frame in this TCP stream: 0.010570000 seconds]
    [Time since previous frame in this TCP stream: 0.000194000 seconds]
  - [SEQ/ACK analysis]
    [iRTT: 0.010376000 seconds]
    [Bytes in flight: 239]
    [Bytes sent since last PSH flag: 239]
    TCP payload (239 bytes)

```

Here we can see,  
 Source port: 51357  
 Destination port: 80  
 Sequence number: 1 which is the number used to ensure the data is received in order  
 Acknowledgment number: 1 which is the number that confirms receipt of the data  
 Len: 239 bytes

## 7. Application Layer

```

Hypertext Transfer Protocol
- GET /MFewTzBNMEswSTA3BgUrDgMcGgUABBTmBSic9rRVLc%2BHKv9a%2FvDh7s6DzAQUgqJwdN28Uz%2FPe9T3zX%2BnYMYKTL8CEA4MdXIURXpChc39PhMRwkQ%3D HTTP/1.1\r\n
- [Expert Info (Chat/Sequence): GET /MFewTzBNMEswSTA3BgUrDgMcGgUABBTmBSic9rRVLc%2BHKv9a%2FvDh7s6DzAQUgqJwdN28Uz%2FPe9T3zX%2BnYMYKTL8CEA4MdXIURXpChc39PhMRwkQ%3D HTTP/1.1\r\n]
  [GET /MFewTzBNMEswSTA3BgUrDgMcGgUABBTmBSic9rRVLc%2BHKv9a%2FvDh7s6DzAQUgqJwdN28Uz%2FPe9T3zX%2BnYMYKTL8CEA4MdXIURXpChc39PhMRwkQ%3D HTTP/1.1\r\n]
  [Severity level: Chat]
  [Group: Sequence]
Request Method: GET
Request URI: /MFewTzBNMEswSTA3BgUrDgMcGgUABBTmBSic9rRVLc%2BHKv9a%2FvDh7s6DzAQUgqJwdN28Uz%2FPe9T3zX%2BnYMYKTL8CEA4MdXIURXpChc39PhMRwkQ%3D
Request Version: HTTP/1.1
Connection: Keep-Alive\r\n
Accept: */*\r\n
User-Agent: Microsoft-CryptoAPI/10.0\r\n
Host: ocsponetrust.net\r\n
\r\n
[Full request URI: http://ocsp.entrust.net/MFewTzBNMEswSTA3BgUrDgMcGgUABBTmBSic9rRVLc%2BHKv9a%2FvDh7s6DzAQUgqJwdN28Uz%2FPe9T3zX%2BnYMYKTL8CEA4MdXIURXpChc39PhMRwkQ%3D]
[HTTP request 1/1]
[response in frame: 15965]

```

Here we can see,  
Method: Get  
URL: maybe this is encrypted  
Request version: HTTP/1.1  
Then header line

## HTTP Response

```

* Frame 15965: 151 bytes on wire (1208 bits), 151 bytes captured (1208 bits) on interface \Device\NPF_{122242F4-49BC-4798-8231-1C1E26995AEF}, id 0
* Ethernet II, Src: TPLink_de:71:a5 (78:8c:b5:de:71:a5), Dst: ASUSTekCOMPU_ae:9f:e9 (c8:7f:54:ae:9f:e9)
* Internet Protocol Version 4, Src: 23.36.25.85, Dst: 192.168.0.5
* Transmission Control Protocol, Src Port: 80, Dst Port: 51357, Seq: 1863, Ack: 240, Len: 97
* [4 Reassembled TCP Segments (1959 bytes): #15961(1270), #15962(479), #15964(113), #15965(97)]
* Hypertext Transfer Protocol
* Online Certificate Status Protocol

```

## 2. Data Link Layer

```

* Ethernet II, Src: TPLink_de:71:a5 (78:8c:b5:de:71:a5), Dst: ASUSTekCOMPU_ae:9f:e9 (c8:7f:54:ae:9f:e9)
  * Destination: ASUSTekCOMPU_ae:9f:e9 (c8:7f:54:ae:9f:e9)
    Address: ASUSTekCOMPU_ae:9f:e9 (c8:7f:54:ae:9f:e9)
    .... ..0. .... = LG bit: Globally unique address (factory default)
    .... ..0. .... = IG bit: Individual address (unicast)
  * Source: TPLink_de:71:a5 (78:8c:b5:de:71:a5)
    Address: TPLink_de:71:a5 (78:8c:b5:de:71:a5)
    .... ..0. .... = LG bit: Globally unique address (factory default)
    .... ..0. .... = IG bit: Individual address (unicast)
  Type: IPv4 (0x0800)

```

This is an IPV4 packet that shows Src and Dst MAC addresses. The Src and Dst are opposite to HTTP requests.

## 3. Network Layer

```

- Internet Protocol Version 4, Src: 23.36.25.85, Dst: 192.168.0.5
  0100 .... = Version: 4
  .... 0101 = Header Length: 20 bytes (5)
  - Differentiated Services Field: 0x20 (DSCP: CS1, ECN: Not-ECT)
    0010 00.. = Differentiated Services Codepoint: Class Selector 1 (8)
    .... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
  Total Length: 137
  Identification: 0x2800 (10240)
  - 000. .... = Flags: 0x0
    0... .... = Reserved bit: Not set
    .0.. .... = Don't fragment: Not set
    ..0. .... = More fragments: Not set
    ...0 0000 0000 0000 = Fragment Offset: 0
  Time to Live: 52
  Protocol: TCP (6)
  Header Checksum: 0x6d29 [validation disabled]
  [Header checksum status: Unverified]
  Source Address: 23.36.25.85
  Destination Address: 192.168.0.5

```

Here we can see IP address, TCP protocol and identification number.

#### 4. Transport Layer

```

Transmission Control Protocol, Src Port: 80, Dst Port: 51357, Seq: 1863, Ack: 240, Len: 97
  Source Port: 80
  Destination Port: 51357
  [Stream index: 143]
  [Conversation completeness: Complete, WITH_DATA (31)]
    ..0. .... = RST: Absent
    ...1 .... = FIN: Present
    .... 1... = Data: Present
    .... .1.. = ACK: Present
    .... ..1. = SYN-ACK: Present
    .... ...1 = SYN: Present
    [Completeness Flags: ·FDASS]
    [TCP Segment Len: 97]
    Sequence Number: 1863      (relative sequence number)
    Sequence Number (raw): 2706886449
    [Next Sequence Number: 1960      (relative sequence number)]
    Acknowledgment Number: 240      (relative ack number)
    Acknowledgment number (raw): 1019411825
    0101 .... = Header Length: 20 bytes (5)
  [Flags: 0x018 (PSH, ACK)]
    000. .... .... = Reserved: Not set
    ...0 .... .... = Accurate ECN: Not set
    .... 0... .... = Congestion Window Reduced: Not set
    .... .0.. .... = ECN-Echo: Not set
    .... ..0. .... = Urgent: Not set
    .... ...1 .... = Acknowledgment: Set
    .... .... 1... = Push: Set
    .... .... .0.. = Reset: Not set
    .... .... ..0. = Syn: Not set
    .... .... ...0 = Fin: Not set
    [TCP Flags: .....AP...]
  Window: 768
  [Calculated window size: 98304]
  [Window size scaling factor: 128]
  Checksum: 0x50d9 [unverified]
  [Checksum Status: Unverified]
  Urgent Pointer: 0
  [Timestamps]
    [Time since first frame in this TCP stream: 0.283081000 seconds]
    [Time since previous frame in this TCP stream: 0.000000000 seconds]
  [SEQ/ACK analysis]
    [iRTT: 0.010376000 seconds]
    [Bytes in flight: 210]
    [Bytes sent since last PSH flag: 97]
  TCP payload (97 bytes)
  TCP segment data (97 bytes)

```

We can see TCP details, port number, Ack no, Seq no etc.

## 7. Application Layer

```

Hypertext Transfer Protocol
HTTP/1.1 200 OK\r\n
  [Expert Info (Chat/Sequence): HTTP/1.1 200 OK\r\n]
    Response Version: HTTP/1.1
    Status Code: 200
    [Status Code Description: OK]
    Response Phrase: OK
    Content-Type: application/ocsp-response\r\n
    ETag: "903CCE04877BABC4B014995BC58C97D000C73DE52FB87E03C9EBFCCC816B5DC4"\r\n
    Last-Modified: Fri, 28 Jun 2024 07:00:00 UTC\r\n
  Content-Length: 1588\r\n
    [Content length: 1588]
    Cache-Control: public, no-transform, must-revalidate, max-age=3594\r\n
    Expires: Fri, 28 Jun 2024 15:28:58 GMT\r\n
    Date: Fri, 28 Jun 2024 14:29:04 GMT\r\n
    Connection: Keep-alive\r\n
  \r\n
  [HTTP response 1/1]
  [Time since request: 0.272511000 seconds]
  [Request in frame: 15957]
  [Request URI: http://ocsp.entrust.net/MFEWtZBNMEswSTAJBgUrDgMCGGUABBTMBSIc9rRVLC%2BHKv9a%2FvDh7s6DzAQUgqJwdN28Uz%2FPe9T3zX%2BnYMYKTL8CEA4MdxIURXpChc39PhMwKwQ%3D]
  File Data: 1588 bytes

```

Here we can see,  
Version: HTTP/1.1  
Status Code: 200  
Phrase: Ok  
Then the header lines.  
Others data

```

Online Certificate Status Protocol
responseStatus: successful (0)
responseBytes
  responseType Id: 1.3.6.1.5.5.7.48.1.1 (id-pkix-ocsp-basic)
  basicOCSPResponse
    tbsResponseData
      responderID: bytename (1)
        producedAt: Jun 28, 2024 13:48:00.000000000 Bangladesh Standard Time
        responses: 1 item
      signatureAlgorithm (sha256withRSAEncryption)
        Algorithm Id: 1.2.840.113549.1.1.11 (sha256withRSAEncryption)
        padding: 0
        signature [truncated]: a0c6efc37a39cdda77b2e9b0988b7766ac1d664886f207ed504d5504894f76eac18e7e1283c6788f08f50f6755ddd486c7b1bd97c2ad2bf6d4271d777a7db2770289150f69ed4e70a93116693a8biac68371a5487a226265c fba503303b54599b60c2848fcd91037c208f8
    certs: 1 item

```

We can also see OCSP (Online Certificate Status Protocol)

128

```
At time +2s client sent 128 bytes to 10.1.1.2 port 9
At time +2.00413s server received 128 bytes from 10.1.1.1 port 49153
At time +2.00413s server sent 128 bytes to 10.1.1.1 port 49153
At time +2.00825s client received 128 bytes from 10.1.1.2 port 9
FlowID: 1 (UDP 10.1.1.1/49153 --> 10.1.1.2/9)
Tx Bytes: 156
Rx Bytes: 156
quot;Tx Packets: 1
quot;Rx Packets: 1
quot;Lost Packets: 0
Mean Delay: 0.0041264
Throughput: 69.33333333333333
FlowID: 2 (UDP 10.1.1.2/9 --> 10.1.1.1/49153)
Tx Bytes: 156
Rx Bytes: 156
quot;Tx Packets: 1
quot;Rx Packets: 1
quot;Lost Packets: 0
Mean Delay: 0.0041264
Throughput: 69.33333333333333
```

256

```
At time +2s client sent 256 bytes to 10.1.1.2 port 9
At time +2.00423s server received 256 bytes from 10.1.1.1 port 49153
At time +2.00423s server sent 256 bytes to 10.1.1.1 port 49153
At time +2.00846s client received 256 bytes from 10.1.1.2 port 9
FlowID: 1 (UDP 10.1.1.1/49153 --> 10.1.1.2/9)
Tx Bytes: 284
Rx Bytes: 284
quot;Tx Packets: 1
quot;Rx Packets: 1
quot;Lost Packets: 0
Mean Delay: 0.0042288
Throughput: 126.22222222222223
FlowID: 2 (UDP 10.1.1.2/9 --> 10.1.1.1/49153)
Tx Bytes: 284
Rx Bytes: 284
quot;Tx Packets: 1
quot;Rx Packets: 1
quot;Lost Packets: 0
Mean Delay: 0.0042288
Throughput: 126.22222222222223
```

512

```
At time +2s client sent 512 bytes to 10.1.1.2 port 9
At time +2.00443s server received 512 bytes from 10.1.1.1 port 49153
At time +2.00443s server sent 512 bytes to 10.1.1.1 port 49153
At time +2.00887s client received 512 bytes from 10.1.1.2 port 9
FlowID: 1 (UDP 10.1.1.1/49153 --> 10.1.1.2/9)
Tx Bytes: 540
Rx Bytes: 540
quot;Tx Packets: 1
quot;Rx Packets: 1
quot;Lost Packets: 0
Mean Delay: 0.0044336
Throughput: 240.0
FlowID: 2 (UDP 10.1.1.2/9 --> 10.1.1.1/49153)
Tx Bytes: 540
Rx Bytes: 540
quot;Tx Packets: 1
quot;Rx Packets: 1
quot;Lost Packets: 0
Mean Delay: 0.0044336
Throughput: 240.0
```

1024

```
At time +2s client sent 1024 bytes to 10.1.1.2 port 9
At time +2.00484s server received 1024 bytes from 10.1.1.1 port 49153
At time +2.00484s server sent 1024 bytes to 10.1.1.1 port 49153
At time +2.00969s client received 1024 bytes from 10.1.1.2 port 9
FlowID: 1 (UDP 10.1.1.1/49153 --> 10.1.1.2/9)
Tx Bytes: 1052
Rx Bytes: 1052
quot;Tx Packets: 1
quot;Rx Packets: 1
quot;Lost Packets: 0
Mean Delay: 0.0048432
Throughput: 467.55555555555554
FlowID: 2 (UDP 10.1.1.2/9 --> 10.1.1.1/49153)
Tx Bytes: 1052
Rx Bytes: 1052
quot;Tx Packets: 1
quot;Rx Packets: 1
quot;Lost Packets: 0
Mean Delay: 0.0048432
Throughput: 467.55555555555554
```

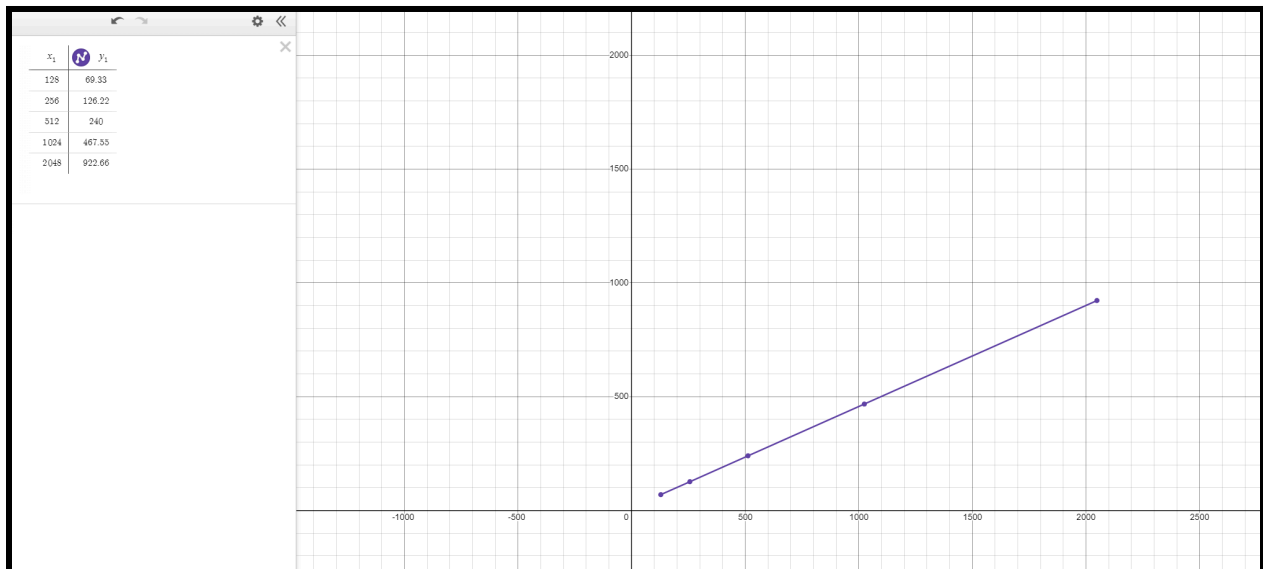
2048



```

At time +2s client sent 2048 bytes to 10.1.1.2 port 9
At time +2.00568s server received 2048 bytes from 10.1.1.1 port 49153
At time +2.00568s server sent 2048 bytes to 10.1.1.1 port 49153
At time +2.01136s client received 2048 bytes from 10.1.1.2 port 9
FlowID: 1 (UDP 10.1.1.1/49153 --> 10.1.1.2/9)
Tx Bytes: 2076
Rx Bytes: 2076
quot;Tx Packets: 1
quot;Rx Packets: 1
quot;Lost Packets: 0
Mean Delay: 0.00568
Throughput: 922.6666666666666
FlowID: 2 (UDP 10.1.1.2/9 --> 10.1.1.1/49153)
Tx Bytes: 2076
Rx Bytes: 2076
quot;Tx Packets: 1
quot;Rx Packets: 1
quot;Lost Packets: 0
Mean Delay: 0.00568
Throughput: 922.6666666666666

```



packet size vs Throughput graph